PERANCANGAN VIRTUAL PRIVATE NETWORK PADA
PT PIKA MEDIA KOMUNIKA

NASKAH PUBLIKASI

disusun oleh

Eling Meyatmaja

10.21.0551

kepada

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

AMIKOM

YOGYAKARTA

2013

NASKAH PUBLIKASI

PERANCANGAN VIRTUAL PRIVATE NETWORK PADA PT. PIKA MEDIA KOMUNIKA

diajukan oleh

Eling Meyatmaja

10.21.0551

Dosen Pembimbing

Melwin Syafrizal, S.Kom, M.Eng

NIK. 190302105

Tanggal, 26 Februari 2013

Ketua Jurusan

Teknik Informatika

STMIK AMIKOM YOGYAKARTA * JURUSAN TI *

Sudarmawan, MT

NIK. 190302035

Desaigning Virtual Private Network Server
At PT Pika Media Komunika

Eling Meyatmaja
Melwin Syafrizal
Jurursan Teknik Informatika
STMIK AMIKOM YOGYAKARTA

ABSTRACT

PT. Pika Komunika Media is a company engaged in the Internet Service Provider who is always attentive to the needs of consumers of security on the internet. But when consumers exchange information there are those who commit the theft of data during transmission on the Internet. Unauthorized parties can freely use and misuse of data for their own purposes. One way to build security in data communication networks is to use the Internet network Virtual Private Network (VPN).

Build and design a VPN server that is placed in one of the customers who can provide a secure VPN connection by forming a tunnel for a point-to-point and do some mechanism to implement security services.

With the construction of a system of data packet delivery and reliable data transfer as there is no data packets are lost during transmission of data.

***Keywords** : OpenVPN, Tunnel, Security Data*

1. Pendahuluan

Teknologi informasi khususnya jaringan komputer menjadi pilhan yang tepat baik itu perusahaan maupun personal untuk menyediakan informasi dan menghubungkann lan ke internet. Hal ini dapat dilihat dari penggunaan internet yang terus meningkat.

PT. Pika Media Komunika adalah perusahaan yang bergerak di bidang Internet Service Provider yang selalu memperhatikan kebutuhan konsumen akan keamanan di internet. Namun ketika konsumen melakukan pertukaran informasi ada pihak yang melakukan pencurian data selama ditransmisikan di internet. Pihak yang tidak berwenang dapat dengan leluasa menggunakan dan menyalahgunakan data untuk kepentingan mereka sendiri. Salah satu cara untuk membangun keamanan komunikasi data dalam jaringan internet adalah dengan menggunakan jaringan Virtual Private Network (VPN).

Teknologi VPN memungkinkan setiap orang untuk dapat mengakses jaringan lokal dari luar menggunakan internet. Dengan menggunakan VPN, maka user dapat mengakses sumber daya yang berada dalam jaringan lokal, mendapatkan hak dan pengaturan yang sama seperti secara fisik berada di tempat dimana jaringan lokal itu berada. Keamanan data dan ketertutupan transmisi data dari akses yang tidak berhak dalam transmisinya pada internet menjadi standart utama dalam VPN, sehingga dalam VPN selalu disertakan akan fitur utama yaitu enkripsi dan tunneling. Alasan tersebut yang mendorong penulis mengambil topik skripsi dengan judul "Perancangan Virtual Private Network Server pada PT . Pika Media Komunika".

2. Landasan Teori

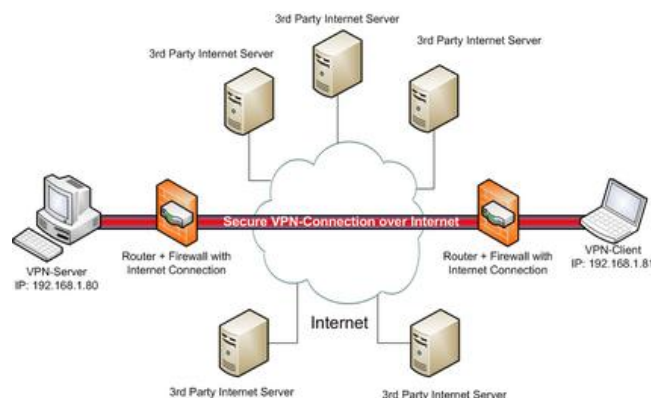
Menurut Priyo Setiawan (2011) Universitas Gadjah Mada Fakultas MIPA dengan judul skripsinya "Implementasi Keamanan Jaringan berbasis OpenVPN". Dalam skripsinya tersebut dijelaskan bahwa OpenVPN dapat memberikan sebuah koneksi VPN yang aman dengan membentuk sebuah tunnel untuk koneksi point-to point dan melakukan beberapa mekanisme untuk mengimplementasikan layanan keamanan dalam OSI , yaitu: enchiperment untuk menjaga kerahasiaan data dalam transmisi, akses control menghindari akses yang tidak berhak terhadap sistem integritas data, akses

kontrol menghindari akses yang tidak berhak terhadap sistem , integritas data , tanda tangan digital yang akan menjaga data agar tidak mengalami perubahan dan menghindari proses pemalsuan.

2.1 Virtual Private Network

2.1.1 Devinisi VPN

> VPN merupakan suatu cara untuk membuat sebuah jaringan bersifat private dan aman dengan menggunakan jaringan public atau internet VPN dapat mengirim data antara dua komputer yang melewati jaringan public yang melewati jaringan public, sehingga seolah-olah terhubung secara point-to point(Mairs,J.2002)[1].

VPN dikembangkan untuk membangun sebuah intranet dengan jangkauan yang luas melalui jaringan internet. Intranet sudah menjadi komponen penting dalam suatu perusahaan dewasa ini. Dengan kata lain, semakin besar permasalahan ini akan semakin kompleks apabila perusahaan tersebut mempunyai banyak kantor cabang yang tersebar di berbagai kota dengan jarak yang jauh. Sedangkan di lain pihak seluruh kantor tersebut memerlukan suatu metode untuk berhubungan misalnya untuk transfer dan sinkronisasi data. Pada mulanya sistem intranet dikembangkan dengan mengunakan sistem dedicated line. Sistem ini menawarkan kecepatan transfer data yang tinggi namun membutuhkan investasi yang mahal system ini tidak efektif untuk perusahaan kelas menengah ke bawah serta perusahaan yang tersebar di berbagai wilayah yang saling berjauhan.

Gambar 2.1 Virtual Private Network
(sumber : http://www.tomshardware.com)

[1] Mairs, J, “VPNs: A Beginner's Guide”, 2002, h208

2.2 Tunneling

2.2.1 Definisi Tunneling

> Tunneling merupakan data yang dienkapsulasi (dibungkus) dengan header yang berisi informasi routing untuk mendapatkan koneksi point to point sehingga data melewati jaringan publik dan dapat mencapai akhir tujuan. Sedangkan untuk mendapatkan koneksi yang bersifat private, data harus dienkripsi terlebih dahulu untuk menjaga kerahasiaannya sehingga paket yang tertangkap ketika melewati jaringan publik tidak terbaca karena harus melewati proses dekripsi(wendy,A., Ramadhana,A., 2005)[2].

Data di transfer dapat berupa frame (paket kecil) dari protocol yang lain. protocol tunneling tidak mengirimkan frame sebagaimana yang dihasilkan oleh node asalnya, melainkan membungkusnya (mengenkapsulasi) dalam header tambahan. header tambahan tersebut berisi informasi routing sehingga data atau frame yang dikirim dapat melewati jaringan internet. Jalur yang dilewati dalam internet tersebut disebut tunnel.

Saat data tiba pada jaringan tujuan , proses yang terjadi selanjutnya adalah dekapsulasi , kemudian dara original akan dikirim ke penerima terakhir. Tunneling mencakup keseluruhan proses mulai dari enkapsulasi , transmisi dan dekapsulasi . Secara umum dalam sebuah proses tunneling, terlibat di dalamnya tiga buah protocol yang berbeda , yaitu:

1. Carrier protocol , ini menjadi protocol yang digunakan oleh jaringan dimana informasi berjalan diatasnya , missal TCP/UDP
2. Encapsulating protocol , protoko ini membungkus data yang asli di dalamnya, missal GRE (Generic Routing Encapsulation) , IP Security (), Layer 2 forwading (L2f), PPTP , atau Layer 2 tunneling protocol (L2TP).
3. Passenger protocol , protocol yang mengangkut data asli dari host pertama kali missal IPX, apple talk atau IP.

---

[2] Aris Wendy, Ahmad SS Ramadhana, “Membangun VPN linux secara cepat”, Penerbit Andi, Yogyakarta 2005, h1

2.3 OpenVPN

2.3.1 Definisi OpenVPN

OpenVPN adalah sebuah solusi VPN yang antar platform , aman dan sangat mudah dikonfigurasikan dengan menggunakan antar muka virtual yang disediakan oleh driver jaringan universal TUN / TAP dan dijalankan sepenuhnya dengan pengguna yang merupakan perlindungan khusus pada sistem(Feilner,M. , 2005)[3].

Keputusan ini dibuat untuk menyediakan keamanan yang lebih baik, karena jika sebuah celah ditemukan oleh penyusup maka aksesnya akan menjadi terbatas. OpenVPN mendukung konfigurasi peer-to-peer dan multiclient yang memungkinkan untuk membuat banyak topologi VPN seperti : host-host , host-network dan network-network . ini mendukung untuk menciptakan VPN layer 3 atau layer 2 dengan menggunakan anatr uka TUN / TAP.

OpenVPN membuat sebuah SSL/TLS session untuk control channel anatr peer, selama fase autentifikasi tiap peer melakukan pertukaran sertifikasi yang di tanda tangani oleh CA (certificate of Authority) yang saling di percaya. Setelah autentikasi selesai dan SSL session telah terbangun di tiap peer , open VPN menggunakan konkesi melakukan negosiasi kunci untuk data channel.

2.4 TUN/TAP

TUN/TAP adalah perangkat point-to-point yang di desain sebagai dukungan untuk level bawah kernel terhadap IP tunneling . TUN menyediakan kepada aplikasi user dua antar muka, yaitu:

1. /dev/tunX, menunjukkan sebagai karakter perangkat.
2. tunX, antarmuka virtual Point to point

Aplikasi dapat menuliskan IP frame pada /dev/tunX dan kernel akan menerima frame tersebut pada antar muka tunX. Pada waktu yang bersamaan setiap frame yang kernel tulis pada antarmuka tunX akan dibaca oleh aplikasi melalui /dev/tunX.

---

[3] Feilner,M. “Building and Integrating Virtual Private Networks”,2006,h28

TAP adalah sebuah perangkat virtual Ethernet yang di desain sebagai dukungan untuk level bawah kernel terhadap Ethernet tunneling. TAP menyediakan kepada aplikasi user dua antar muka , yaitu :

1. /dev/tapX, menunjukkan sebagai karakter perangkat
2. tapX, antar muka virtual Ethernet

2.4 SSL /TLS

2.4.1 Definisi SSL /TLS

Secure Socket Layer (SSL) adalah protocol yang digunakan untuk browsing web secara aman. Dalam hal ini , SSL bertindak sebagai protocol yang mengamankan komunikasi antara client dan server. Protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara website dan web browser (Munir, R. 2004)[4]

SSL dikembangkan oleh Netscape Communication pada tahun 1994 , dan menjadi protocol yang umum digunakan untuk komunikasi aman anatara dua computer pada internet. SSL dibangun ke dalam banyak web browser (termasuk NETscape Communicator dan Internet Explorer). Ada beberapa versi SSL , versi 2 dan versi 3 , tetapi versi 3 paling banyak digunakan saat ini.

SSL yang dikembangkan oleh pada tahun 1994 sampai sekarang sudah mencapai versi tiga. Pada tahun 1996 Netscape Communication Corp mengajukan SSL ke IETF (*Internet Engginering Task Force*) untuk melakukan standarisasi. Hasilnya adalah TLS (*Transport Layer Security*) yang dijelaskan RFC 2246, TLS dapat dianggap sebagai SSL versi 3.1 dan implementasi kan pertama pada tahun 1999.

3. Analisis Masalah

PT Pika Media Komunika memiliki klien yang terdiri dari perusahaan 60 korporasi, 4 instansi , 2 bisnis maupun personalan. Beberapa bulan ini ada permintaan akan layanan VPN. Setiap klien membutuhkan layanan yang berbeda-beda seperti korporasi dan instansi pemerintahan yang membutuhkan layanan dengan kebutuhan

---

[4] Munir,R.” Bahan Kuliah ke 26 IF5054 Kriptografi”,2004

jalur khusus. Kegiatan klien instansi pemerintah dan bisnis yang mengirim dan menerima data, yang berarti transaksi data yang terjadi setiap hari. Terutama klien perusahaan yang sedang berkembang dan memiliki banyak kantor cabang dan sering melakukan komunikasi dengan kantor cabangnya tersebut. Komunikasinya bisa berupa pertukaran data, informasi dan lain-lain. Terkadang informasi yang dipertukarkan merupakan informasi yang bersifat rahasia. Data-data transaksi dikirim dengan menggunakan internet melalui messenger dan email. Dengan hanya menggunakan media tersebut, keamanan data yang dikirim atau diterima rentan terhadap pencurian ,rusak, atau hilang.

3.1 Solusi Masalah

Berdasarkan hasil permasalahan yang dihadapi, maka diusulkan pemecahan masalah dengan cara membuat *Virtual Private Network* (VPN). Dengan VPN maka klien dan seluruh cabang-cabangnya dapat dihubungkan menjadi satu jaringan intern dengan menggunakan media jaringan publik/ jaringan internet yang ada sebagai media perantara. Selain kantor cabang, semua karyawan dan staff yang kebetulan sedang tidak dapat berada di perusahaan tetapi ingin mengakses data pekerjaan atau data-data yang diinginkan dapat mengaksesnya melalui jalur internet.

Penggunaan internet sebagai media VPN dapat menekan biaya yang dikeluarkan dan lebih mudah untuk diterapkan daripada membuat sebuah jaringan baru menggunakan media kabel ataupun wireless. Pemilihan jenis VPN yang akan digunakan tentu saja harus memiliki sistem keamanan yang baik agar semua data yang melewatinya tidak jatuh ke orang-orang yang tidak berhak untuk mengakses data tersebut. Selain pada sisi keamanan, VPN yang akan digunakan juga harus menyediakan kemudahan kepada administrator dalam melakukan konfigurasi, administrasi.

3.2 Analisis Kebutuhan

3.2.1 Analisis Kebutuhan Perangkat Keras

Analisis perangkat keras meliputi aspek hardware yang dipakai dalam pembuatan dan instalasi server VPN. Pada penelitian ini komputer server yang digunakan sebagai server VPN memiliki speseifikasi sebagai berikut:

1. Prosesor : Procecor Intel (R) Pentium 4 CPU 1.8GHz
2. Memory : 256mb
3. Hardisk : 20GB
4. VGA : Nvidia NV11(geforce2 MX/MX 400)
5. Lan Card : Realtek RTL8139/810x Family Fast Ethernet NIC

3.2.2 Analisis Kebutuhan Perangkat Lunak

Analisis perangkat lunak meliputi aspek software yang dipakai atau mendukung dalam pembuatan dan analisis server VPN , server VPN dibangun dengan menggunakan Sistem Operasi Linux Ubuntu 12.04 yang berbasis distro debian. adapun aplikasi pendukung yang dipakai antara lain :

1. Sistem operasi Ubuntu 12.04, dengan alamat http://www.ubuntu.com/download/server
2. Aplikasi OpenVPN untuk membuat jaringan pribadi antara VPN server dan VPN klien, dengan alamat URI : http://openvpn.net/index.php/download.html
3. Software Putty untuk remote server ubuntu 12.04 http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
4. WinSCP adalah aplikasi open source klien SFTP, SCP ataupun FTP di Windows. Fungsi utamanya adalah menyediakan sarana pengiriman data yang aman antara komputer lokal dan komputer remote. http://winscp.net/eng/download.php#download2

3.2.3 Perangkat Manusia (Brainware)

Sistem ini dibangun dapat dikelompokkan menjadi dua level pengguna yang akan memanfaatkan sistem ini yaitu adminstrator dan user .

1.Administrator

Admin mempunyai hak penuh untuk melihat , menambah , mengubah menghapus data atau informasi yang ada di sistem yang memiliki keahlian pemahaman konsep akan jaringan dan linux yang itu akan membantu dalam menghadapi troubleshoot ketika sistem tidak berjalan dengan baik.

2.User

Pengguna layanan OpenVPN harus bisa memahami konsepnya sehingga ketika user ingin melakukan transfer data dapat dari server ke client maka dari itu hak akses yang diberikan oleh admin sesuai dengan batasan sistem yang dikehendaki. User disini yaitu para pelanggan yang memakai jasa dari perusahaan tersebut

.3.3 Analisis Biaya

Biaya untuk membangun Virtual Private Network (VPN) dengan memanfaatkan investasi hardware yang masih layak digunakan sebagai server VPN yang dimiliki oleh klien.

Biaya software operasi sitem bersifat open-source yaitu ubuntu 12.04 dan VPN sendiri dari sekian banyak software VPN yang beredar dipilih sebuah software yang bersifat open-source yang bernama OpenVPN yang memiliki banyak keunggulan seperti yang telah disebutkan di atas. OpenVPN ini dipilih karena menggunakan dua buah *cryptosystem* sebagai metode enkripsinya yaitu *symmetric cryptosystem* dan *asymmetric cryptosystem* SSL/TLS dan *Diffie Hellman* pada saat pertukaran key untuk proses *handshake* koneksi VPN. Hal ini membuat OpenVPN memiliki keamanan yang baik. Berikut daftar kebutuhan dalam membangun VPN server.

NO	Jenis Kebutuhan	Total Investasi
1	CPU SERVER	Rp 0-
2	Bandwith koneksi 1M	Rp 1.300.000
3	Ubuntu 12.04	Free (open source)
4	WinSCP	Free Download
5	Putty	Free Download

4. Hasil Penelitian Dan Pembahasan

Langkah pertama adalah mengecek sistem alamat sistem jaringan. Pengujian konektifitas dilakukan dengan menggunakan ifconfig.

```
root@vpn:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:e0:4d:47:ae:65
          inet addr:192.168.20.221  Bcast:192.168.20.255  Mask:255.255.255.0
          inet6 addr: fe80::2e0:4dff:fe47:ae65/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47052 errors:0 dropped:0 overruns:0 frame:0
          TX packets:39859 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21551809 (21.5 MB)  TX bytes:21052111 (21.0 MB)
          Interrupt:23 Base address:0x8000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:104 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:8052 (8.0 KB)  TX bytes:8052 (8.0 KB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:13660 errors:0 dropped:0 overruns:0 frame:0
          TX packets:20147 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:1355306 (1.3 MB)  TX bytes:17057570 (17.0 MB)
```

Gambar 4.18 Ifconfig pada server VPN

Pada gambar diatas dapat dilihat kalau server memiliki interface tun0 dengan IP 10.8.0.1 yang diberikan oleh OpenVPN. Sedangkan interface eth0 digunakan untuk melakukan koneksi ke internet.

4.2.1 Proses Koneksi dari Client ke Server

Setelah tahap instalasi dan konfigurasi server dan client selesai maka tahap selanjutnya adalah menjalankan service server OpenVPN pada server dan client.

4.2.2.1 Menjalankan OpenVPN pada Server

Berikut ini adalah proses pengoperasian service server OpenVPN :

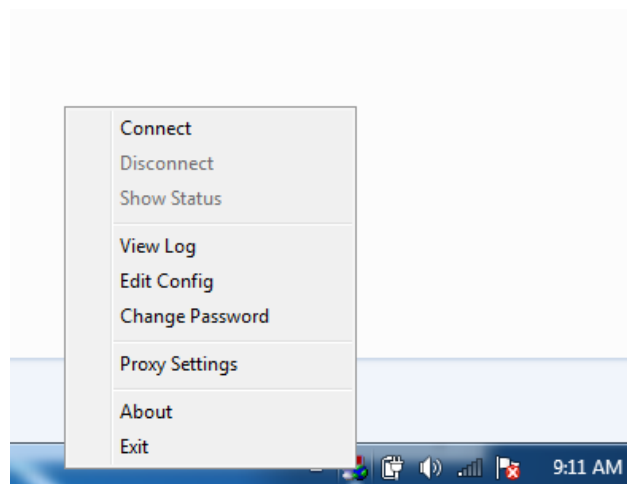
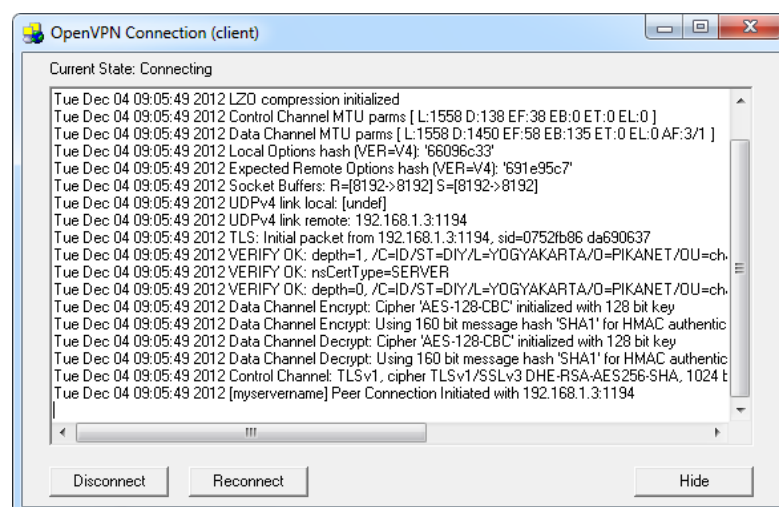
```
root@vpn:/etc/init.d/openvpn restart
```

melakukan restart pada server OpenVPN.

```
root@vpn:~# /etc/init.d/openvpn start
 * Starting virtual private network daemon(s)...
 *   Autostarting VPN 'server'
root@vpn:~#
```

Gambar 4.19 Service OpenVPN dijalankan

4.2.2.2 Menjalankan OpenVPN pada client

Setelah konfigurasi selesai dilakukan maka apabila melakukan klik kanan pada OpenVPN GUI di taskbar akan muncul pilihan koneksi pada OpenVPN GUI di taskbar seperti gambar di bawah ini.

Gambar 4.20 Ada Pilihan Connect pada Client

Gambar 4.21 Proses Koneksi dari client ke server

Gambar 4.22 Client connect dengan server

4.2.2 Sebelum dan sesudah diaktifkan OpenVPN

1. Melakukan pengujian VPN server melalui tunneling yaitu dengan menggunakan ping dari client ke server sebelum dan sesudah diaktifkan OpenVPN server

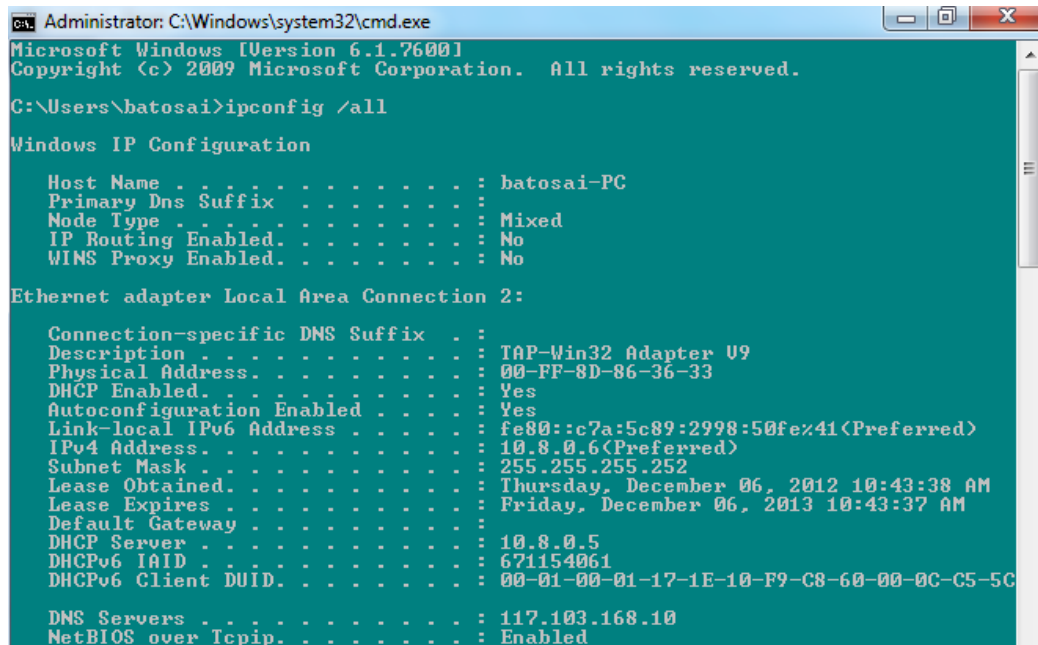
```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\batosai>ping 10.8.0.1

Pinging 10.8.0.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.8.0.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\batosai>
```

Gambar 4.23 Sebelum diaktifkan OpenVPN server

```
C:\Users\batosai>ping 10.8.0.1

Pinging 10.8.0.1 with 32 bytes of data:
Reply from 10.8.0.1: bytes=32 time=154ms TTL=64
Reply from 10.8.0.1: bytes=32 time=285ms TTL=64
Reply from 10.8.0.1: bytes=32 time=132ms TTL=64
Reply from 10.8.0.1: bytes=32 time=113ms TTL=64

Ping statistics for 10.8.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 113ms, Maximum = 285ms, Average = 171ms
```

Gambar 4.24 sesudah diaktifkan OpenVPN server

2. Melihat status konfigurasi interface client, untuk melihat konfigurasi pada client windows dengan perintah ipconfig /all setelah terhubung ke VPN server

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\batosai>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : batosai-PC
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Mixed
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : TAP-Win32 Adapter V9
   Physical Address. . . . . . . . . : 00-FF-8D-86-36-33
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::c7a:5c89:2998:50fe%41(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.8.0.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.252
   Lease Obtained. . . . . . . . . . : Thursday, December 06, 2012 10:43:38 AM
   Lease Expires . . . . . . . . . . : Friday, December 06, 2013 10:43:37 AM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 10.8.0.5
   DHCPv6 IAID . . . . . . . . . . . : 671154061
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-17-1E-10-F9-C8-60-00-0C-C5-5C

   DNS Servers . . . . . . . . . . . : 117.103.168.10
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Gambar 4.25 Ethernet adapter local area connection 2

Terlihat pada saat proses transfer data tipe paket data ketika sebelum mengaktifkan OpenVPN yang ditransfer adalah berupa protocol TCP yang lebih mementingkan keakuratan.

Sedangkan ketika sesudah diaktifkan OpenVPN protocol yang digunakan adalahProtokol UDP dipilih karena prinsipnya yang mementingkan kecepatan akan menambah kecepatan transfer data melewati VPN.

Setelah melakukan evaluasi dari berbagai aspek terhadap perancangan dan implementasi sistem yang telah dibuat, hasilnya adalah sebagai berikut:

1. Konfigurasi server dan klien berjalan dengan baik.
2. Server VPN yang berada di jaringan local dapat dicapai oleh klient.
3. Tunnel OpenVPN berjalan dengan baik dan bekerja pada kedua arah.
4. Tunnel OpenVPN dapat diandalkan (reliable) karena tidak ada paket data yang hilang saat pengiriman data

5. Kesimpulan

Setelah melakukan analisis serta uji coba dan simulasi Virtual Private Network (VPN) seperti yang telah dijelaskan pada bab-bab sebelumnya, maka dapat disimpulkan sebagai berikut :

1. Dengan menggunakan Linux Ubuntu 12.04 sebagai server VPN untuk membangun sebuah jaringan private dan membentuk tunneling untuk koneksi point to point agar mudah dalam pengiriman data dan server terbut dimplementasikan di client yang membutuhkan jalur khusus untuk proses pertukaran data.
2. Penerapan VPN diletakkan di client dengan kebutuhan jalur khusus dengan melakukan koneksi dari client ke server sehingga terbentuk koneksi point to point.
3. OpenVPN dapat ditinjau keamanannya dari proses pengiriman dan transfer data dari server ke client.
4. Menurut hasil uji coba sistem OpenVPN dapat disimpulkan sebagai berikut :
    a) Konfigurasi server dan klien berjalan dengan baik
    b) Server VPN yang berada di jaringan local dapat dicapai oleh klient.
    c) Tunnel OpenVPN berjalan dengan baik dan bekerja pada kedua arah.
    d) Tunnel OpenVPN dapat diandalkan (reliable) karena tidak ada paket data yang hilang saat pengiriman data.

DAFTAR PUSTAKA

Aris W, Ramadhana A. 2005. *Membangun VPN linux secara cepat*. Yogyakarta : Andi.

Feilner,M. 2006. *Building and Integrating Virtual Private Networks.*

Mairs, J. 2002. *VPNs: A Beginner's Guide*.

Munir,R. 2004. *Bahan Kuliah ke 26 IF5054 Kriptografi*.